Department of
INFORMATION
TECHNOLOGY

Maryland Security Assessment Policy

Last Updated: 01/31/2017

Contents

1.0 Purpose

The Maryland Department of Information Technology (DoIT) is responsible for, and committed to, managing the confidentiality, integrity, and availability of State government information technology (IT) networks, systems, and applications within the scope of its authority. This policy sets standards for Risk Assessment, Vulnerability Assessment, and Penetration Testing as an overall approach to mitigating exploitation and data compromise posed by cyber attackers and vulnerabilities.

This policy mandates DoIT to evaluate risk within the DoIT Enterprise and determine how to eliminate, mitigate, or accept those risks. DoIT will utilize the baseline controls and standards established by NIST SP 800-53R4, SP 800-53AR4, SP 800-30R1, SP 800-115, and FIPS Publication 199 to develop its security assessment requirements and to categorize assets.

2.0 Document and Review History

This policy supersedes the Maryland Information Security Policy v3.1 (2013), Section 5: Management Level Controls and any related policy regarding security assessment declared prior to the 2017 Cybersecurity Program Policy. This document will be reviewed annually and is subject to revision.

Date	**Version**	**Policy Updates**	**Approved By:**
01/31/2017	v1.0	Initial Publication	Maryland CISO

3.0 Applicability and Audience

This policy is applicable to all IT environments and assets owned or operated by any agency supported by, or under the policy authority of, the Maryland Department of Information Technology. DoIT will be responsible for determining risk, developing the security assessment processes in accordance with the requirements in this policy, and providing assessment guidance to non-Enterprise agencies managing IT assets. Agencies under the policy authority, but not under direct management of DoIT, must independently comply with the requirements of this policy.

4.0 Policy

This policy mandates the requirements for conducting security assessments within the DoIT Enterprise. Performing proper risk assessments is the foundation of the DoIT Cybersecurity Program Plan. Managing risk ensures that all agency and third-party connections comply with established standards and that processes are in place to mitigate the risks of these interconnections. Vulnerability analysis and penetration testing are proactive defensive methods for assessing the current DoIT Enterprise security posture.

4.1 General Requirements

#	Name	Requirement
A	Asset Security Categorization	Agencies shall assign all **Information Technology Assets** a security category in accordance with section 4.2 of this policy.
B	Risk and Security Assessments	Agencies shall use risk and security assessments in accordance with the requirements in this document.
C	Confidentiality of Results	All assessment results will be considered confidential information, and will only be released to agency cyber security and IT management. Those individuals must authorize the release of results to any other parties.
D	Categorization of Results	All assessment results will be considered confidential information and will be protected in accordance with the DoIT *Public and Confidential Information Policy*.
E	Tool Approval	All tools used for technical security assessments must be approved by: ▪ State CISO (if Enterprise onboarded); or ▪ Designated, non-Enterprise agency authority (if not actively managed by DoIT).
F	Personnel Approval	All personnel assigned to conduct security assessments must be approved by: ▪ State CISO (if Enterprise onboarded); or ▪ Designated, non-Enterprise agency authority (if not actively managed by DoIT).

4.2 Asset Security Categorization

Determining an asset’s security category requires assessment of the potential impact of events to an IT asset that may jeopardize its confidentiality, integrity, and availability and prevent an agency from accomplishing its business or mission functionality.

- Security categories should be used in conjunction with vulnerability and threat information to assess the risk to an agency
- Agencies must assess and categorize all IT assets to fully comply with the *Asset Management Policy*

NOTE: The categorization of an asset or system may be impacted by the information it stores or processes, and the *information* may drive the security categorization of an asset.

Agencies will use the security categorizations as described in FIPS Publication 199 to categorize assets. The categories are listed below and described in further detail in the following sub-sections:

- LOW
- MODERATE
- HIGH

4.2.1 Low Categorization

The potential impact is LOW — if the loss of confidentiality, integrity, or availability could be expected to have a LIMITED ADVERSE EFFECT on organizational operations, organizational assets, or individuals.

Clarification: A limited adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced; (ii) result in minor damage to agency assets; (iii) result in minor financial loss; or (iv) result in minor harm to individuals.

4.2.2 Moderate Categorization

The potential impact is MODERATE — if the loss of confidentiality, integrity, or availability could be expected to have a SERIOUS ADVERSE EFFECT on organizational operations, organizational assets, or individuals.

Clarification: A serious adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a significant degradation in mission capability to an extent and duration that the agency is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; (ii) result in significant damage to agency assets; (iii) result in significant financial loss; or (iv) result in significant harm to individuals that does not involve loss of life or serious life threatening injuries.

4.2.3 High Categorization

The potential impact is HIGH — if the loss of confidentiality, integrity, or availability could be expected to have a SEVERE OR CATASTROPHIC ADVERSE EFFECT on agency operations, organizational assets, or individuals.

Clarification: A severe or catastrophic adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a severe degradation in or loss of mission capability to an extent and duration that the agency is not able to perform one or more of its primary functions; (ii) result in major damage to agency assets; (iii) result in major financial loss; or (iv) result in severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries.

4.3 Primary Assessment Types

Agencies will deploy multiple types of assessment. These types are listed below and described in further detail in the following sub-sections:

- Organization-wide Risk Assessment
- Targeted Risk Assessment
- System Security Plan (SSP)

4.3.1 Organization-wide Risk Assessment

Each agency shall maintain an **Organization-wide Risk Assessment**. If multiple agencies share IT resources or a directly-networked environment, they shall be treated as a single organization and require a single organization-wide risk assessment that evaluates the agencies as a single entity with multiple stakeholders. Assessment requirements are listed in the table below.

#	Name	Requirement
A	Role	DoIT shall designate an Enterprise **Risk Manager** who will be responsible for the management and enforcement of the Risk Assessment requirements of this policy. Non-Enterprise agencies handling their own Risk Assessment must similarly designate an agency authority to manage and enforce the Risk Assessment requirements of this policy.
B	Standards-based	Risk Assessments will be conducted in accordance with the assessment guidance found within NIST SP800-30, "Risk Management Guide". NOTE: The NIST guide includes an appendix of discrete threat events. For purposes of expediency and realism, it is permissible to create scenarios that represent combinations of these threat events, rather than measure each discrete event separately.
C	Primary Contributing Measures and Data	Risk measures will be generated based upon the results of: ▪ Identifying agency assets and assigning them to security categories ▪ Assessing cyber threats ▪ Assessing vulnerabilities ▪ Assessing likelihood of occurrences ▪ Assessing impact of occurrences
D	Reporting Recipients	For all Executive Branch agencies, the following leadership will receive the results of all Organization-wide Risk Assessments: ▪ Secretary of IT ▪ State Chief Operations Officer ▪ State Chief Information Security Officer ▪ DoIT Enterprise Risk Manager ▪ For non-Enterprise agencies, results will also be reported to the agency's executive leadership, to include the Deputy CIO.
E	Update Cadence	The Organization-wide Risk Assessment shall be updated every 3 years.
F	Conditional Updates	The Organization-wide Risk Assessment shall additionally be updated when the following conditions occur: ▪ An agency combines with, or absorbs another agency, either entirely or for the purposes of IT management ▪ A new IT environment is deployed within the agency, for example a new major facility or sub-organization ▪ The agency's current environment undergoes a major re-architecture ▪ For any other reason, as required by the State CISO or delegated authority
G	Assessment Process	DoIT will establish and provide a high level process guide for conducting an organization-wide risk assessment.

#	Name	Requirement
H	Forms and Templates	DoIT will create and provide standardized forms and templates that can be used to uniformly document risk assessment results.

4.3.2 Targeted Risk Assessment

Conditions for Usage

Targeted risk assessments shall be used to measure risk on environments smaller than an entire agency or organization, in accordance with the conditions described in the table below.

#	Name	Conditions
A	Acquisition of an Agency or Organization	If an agency acquires another state agency or organization, and assumes responsibility for that organization’s information technology, then a targeted assessment will be conducted for the organization being acquired.
B	New Environment Build	Agencies that create new IT environments, for example, deploying a major new network segment or new facility, will conduct a targeted risk assessment on that new environment.
C	Re-Architect Current Environment	If an agency makes fundamental architecture changes to its current environment, it will conduct a targeted risk assessment of the new architecture.
D	Other	Any other circumstance as deemed necessary by the State CISO or delegated authority.

Requirements

Targeted risk assessments will be conducted in accordance with the following requirements.

#	Name	Conditions
E	Equivalent Requirements from Organization-wide Risk Assessment	Targeted risk assessments will comply with all requirements of organization-wide risk assessments (See Section 4.3.1*)*, with the following exceptions: ▪ Targeted Assessments may not require Conditional Updates at a later time. ▪ Targeted Assessments may, where appropriate, utilize sub-section results (Threat, Impact, etc.) from the broader Organization-wide Risk Assessment, rather than duplicate work.
F	Update to Organization-wide Risk Assessment	Upon completion of the targeted risk assessments, assessment results will be used to update the organization-wide risk assessment.

4.3.3 System Security Plan

Conditions for Usage

A **System Security Plan (SSP)** is used to assess the security posture of a given information system or network of systems in order to determine whether or not that system or network can be granted an **Authority to Operate (ATO)**, or as part of externally imposed certification and accreditation requirements (See *Cybersecurity Authority to Operate Policy)*. SSPs are required when the circumstances listed in the table below arise.

#	Name	Condition
A	Device Configuration Standard	A new configuration standard is created for a device type (workstation, server, router, etc.)
B	Operating System Configuration Standard	A new configuration standard is created for an operating system
C	Application Configuration Standard	A new configuration standard is created for an application
D	Non-conforming Deployment	A device, operating system, or application is deployed in a manner that is known to be non-conformant with configuration standards
E	Network Segment	One or more network segments are established
F	3rd Party Connection	A connection is established between the agency and a third party; may be one of several types of connections, including, but not limited to: ▪ Wide Area Network (WAN) ▪ Virtual Private Network (VPN) ▪ Application-to-application ▪ Cloud/externally-hosted application
G	Internet Connection	A new connection is established between the agency and the Internet

Requirements

An SSP must be submitted by the system or network owner to the **Designated Approval Authority (DAA)** and will utilize the template available in NIST SP800-18R1, Appendix A, and must have the minimum requirements listed in the table below.

#	Name	Requirement
H	Information System Identity	Indicate the unique identifier and name given to the system.
I	Information System Owner Contact Details	▪ Name, title, agency, address, email address, and phone number of person who owns the system ▪ Other key personnel, if applicable; include their title, address, email address, and phone number
J	Assigned Risk Category	Identify the appropriate FIPS 199 categorization.
K	Operational Type and Status	Indicate the operational type, such as general support or application server, and the status of the system.
L	Information System Purpose	Describe the function or purpose of the system and the information processes.
M	Other Interconnections	▪ List any interconnected systems and system identifiers (if appropriate) and provide the system, name, organization, system type. ▪ Indicate if there is an ISA/MOU/MOA on file, date of agreement to interconnect, FIPS 199 category, C&A status, and the name of the authorizing official.
N	Implemented Security Controls	Select the appropriate minimum security control baseline (low-, moderate-, high-impact) from NIST SP 800-53, then provide a thorough description of how all the minimum security controls in the applicable baseline are being implemented or planned to be implemented.

4.4 Supporting/Secondary Assessment Types

The following secondary assessment types, may be included within primary assessment types identified above, and have additional requirements listed below.

- Vulnerability assessments
- Penetration tests

4.4.1 Vulnerability Assessments

Vulnerability assessments are intended to provide an accurate and thorough identification of the known vulnerabilities in an information system or set of systems. These assessments may be conducted to supplement risk assessments or SSPs, and will be conducted in accordance with the following requirements.

#	Name	Requirement
A	Processes	DoIT will establish and document vulnerability assessment processes.
B	Standards-based	DoIT will consider industry standards when creating vulnerability assessment processes, including NIST SP 800-115 "Technical Guide to Information Security Testing and Assessments".
C	Vulnerability Conventions	DoIT will establish and document conventions for naming vulnerabilities and assigning severity, and will make these conventions available to all agencies.
D	Authorization to Proceed	All vulnerability assessments will require authorization from the agency's Designated Approval Authority (DAA). NOTE: The DAA may issue a single authorization for an assessment, or a blanket approval for multiple assessments to be conducted at regular intervals.
E	Scheduling	All vulnerability assessments must occur within pre-defined and approved time frames.
F	Notifications	Agency security staff and the DoIT SOC shall be made aware of all assessment targets, and the dates and times when those targets will be accessed and scanned.
G	Contact Line	Agencies security staff and vendors will maintain a direct line of communication during all periods of vulnerability assessment for status updates and reporting of issues.
H	Staff Authorization	Individual staff members must be specifically authorized and qualified to use vulnerability assessment tools.
I	Authenticated Scanning	▪ Agencies will make credentials available to security staff for authenticated scanning wherever possible ▪ Credentials provided for this use will be protected in accordance with all security policies
J	Reporting	All findings will be reported promptly to staff responsible for vulnerability remediation for the agency.
K	Additional Limitations	Non-State of Maryland systems shall never be scanned.

4.4.2 Penetration Testing

Penetration testing will comply with the requirements listed in the table below.

#	Name	Requirement
A	Authorization to Proceed	Every penetration test engagement must be approved by the agency's cyber security DAA.
B	Testing Monitors	One security staff member and one IT staff member will be appointed as Testing Monitors to monitor each penetration test. Penetration testing staff will update these Testing Monitors with regards to testing activities once per day, when applicable.
C	Target Authorizations	All individual target devices, applications, and accounts must be cleared by Testing Monitors before any exploits are launched against these targets.
D	Scheduling	All penetration testing must occur within pre-defined and approved time frames.
E	Notifications	Agency security staff and the DoIT SOC shall be made aware of all testing times and targets. EXCEPTION: Unannounced penetration tests may be conducted, but only with approval by the Secretary of IT.
F	Contact Line	Agencies security staff and vendors will maintain a direct line of communication during all periods of penetration testing for status updates and reporting of issues. EXCEPTION: Unannounced penetration tests may be conducted, but only with approval by the Secretary of IT.
G	Staff Authorizations	▪ Individual staff members must be specifically authorized to use penetration testing tools ▪ Staff members must pass a background check in order to be approved to use penetration testing tools ▪ Staff members must have at least 2 years of direct experience conducting penetration tests before they can be authorized to perform penetration testing activities against production systems at the agency ▪ Vendors and contracting companies must attest that their staff have met the requirements above
H	Network Traffic Capture	All penetration testing events will be logged and made available for post-test auditing.
I	Additional Limitations	Penetration testing tools and techniques shall never be used against non-State of Maryland systems.

5.0 Exemptions

This policy is established for use within the DoIT Enterprise. If an exemption from this policy is required, an agency needs to submit a DoIT Policy Exemption Form and clearly articulate the reason for the exemption. An operational risk assessment will be conducted to identify the risks and the agency's mitigation strategy associated with this exemption. If the agency can accept the risk, an exemption to this policy may be granted.

6.0 Policy Mandate and References

The Cybersecurity Program Policy mandates this policy. Related policies include:

- Asset Management Policy
- Cybersecurity Authority to Operate Policy
- Third Party Interconnection Policy

7.0 Definitions

Term	Definition
Authority to Operate	Authority granted to an information system, by a Designated Approving Authority (DAA), to be used in accordance with its intended purpose within agency IT environments. An ATO authorizes operation of a Business Product and explicitly accepts the risk to agency operations.
Designated Approval Authority (DAA)	Official with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals. Responsible for signing Authority to Operate (ATO), Interim Authority to Operate (IATO), and associated Third-Party Interconnection Agreements.
Information Technology Assets	The collection of Information Technology systems critical to the mission and business functionality of the State of Maryland Executive Branch. Assets typically include physical devices such as servers, virtual servers, desktop workstations, laptops, printers/scanners, VoIP systems, telecomm assets, security (such as CCTV or entry control systems), and offline or SCADA-type systems; software such as purchased applications and programs, associated licenses; and data, such as information or aggregate digital content processed, stored, or transmitted by IT systems, which include agency mission/business data, classified or sensitive data such as PII, or database content.
Organization-wide Risk Assessment	The process of identifying, prioritizing, and estimating risks. This includes determining the extent to which adverse circumstances or events could impact an enterprise. Uses the results of threat and vulnerability assessments to identify risk to organizational operations and evaluates those risks in terms of likelihood of occurrence and impacts if they occur.
Penetration Tests	A test methodology in which assessors, typically working under specific constraints, attempt to circumvent or defeat the security features of an information system.
Risk Manager	Official authority within DoIT or non-Enterprise agency responsible for managing and enforcing compliance with the Risk Assessment portion of this policy and associated processes.
System Security Plan (SSP)	Formal document that provides an overview of the security requirements for an information system and describes the security controls in place or planned for meeting those requirements.
Targeted Risk Assessment	An information system, part of a system or product, and all associated documentation that is the subject of a security evaluation.
Vulnerability Assessments	Systematic examination of an information system or product to determine the adequacy of security measures, identify security deficiencies, provide data from

Term	Definition
	which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation.

8.0 Enforcement

The Maryland Department of Information Technology is responsible for managing security assessments for the DoIT Enterprise according to established requirements authorized in the DoIT Cybersecurity Program Policy. Agencies not directly managed by DoIT must exercise due diligence and due care to comply with the minimum standards identified by the relevant DoIT policies. Any agencies under the policy authority of DoIT with requirements that deviate from the DoIT Cybersecurity Program policies are required to submit a Policy Exemption Form to DoIT for consideration and potential approval.

If DoIT determines that an agency is not compliant with this policy, the agency will be given a sixty (60) day notice to become compliant or at least provide the DoIT a detailed plan to meet compliance within a reasonable time before the issue is reported to the Secretary of Information Technology. After which, the Secretary of Information Technology, or a designated authority, may extend a non-compliant agency's window of resolution or revoke an agency or third-party's authority to operate on DoIT resources until such time the agency becomes compliant.

Any attempt by personnel to circumvent or otherwise bypass this policy or any supporting policy will be treated as a security violation and subject to investigation. The results of the investigation may entail written reprimand, suspension, termination, and possibly criminal and/or civil penalties.